FortiGate NIDS 指南

FortiGate 用户手册 第四卷

版本 2.50 MR2
2003 年 8 月 6 日

© Copyright 2003 美国飞塔有限公司版权所有。

本手册中所包含的任何文字、例子、图表和插图，未经美国飞塔有限公司的许可，不得因任何用途以电子、机械、人工、光学或其它任何手段翻印、传播或发布。

FortiGate NIDS 指南
版本 2.50 MR2
2003 年 8 月 8 日

注册商标
本手册中提及的产品由他们各自的所有者拥有其商标或注册商标。

服从规范
FCC Class A Part 15 CSA/CUS

请访问 http://www.fortinet.com 以获取技术支持。

请将在本文档或任何 Fortinet 技术文档中发现的错误信息或疏漏之处发送到 techdoc@fortinet.com。

目录

概述 1

NIDS 模块 1
　使用 NIDS 检测模块检测入侵企图 1
　使用 NIDS 预防模块预防入侵 1
　使用 NIDS 响应模块管理消息 2
NIDS 检测和预防特性 2
　拒绝服务 (DoS) 攻击 2
　嗅探 2
　权利提升 3
　NIDS 躲避 3
关于本文档 3
2.50 版中的新增内容 3
文档约定 4
Fortinet 的文档 5
　Fortinet 技术文档的注释 5
客户服务和技术支持 6

检测攻击 7

特征组 7
特征举例 9
一般配置步骤 11
NIDS 常规配置 11
　选择要监视的网络接口 11
　禁用 NIDS 11
　配置校验和检验 12
选择一个特征组 12
　查看特征列表 12
　启用和禁用 NIDS 攻击特征 13
更新攻击定义 14

创建用户定义的特征 15

创建用户自定义的特征 15
　用户定义特征提示 17
常规配置步骤 17
用户定义特征的语法 17
　语法约定 17
　完整的特征语法 17
　特征语法的细节 19
管理用户定义的特征 24
　上载用户定义特征列表 24
　下载用户定义特征列表 24

预防攻击 25

一般配置步骤 26
启用 NIDS 攻击预防 26
启用 NIDS 预防特征 27
配置特征临界值 31
配置 syn 淹没特征值 32
举例：NIDS 配置 33
预防 TCP 和 UDP 攻击 33

管理 NIDS 消息 37

记录攻击消息日志 37
配置 FortiGate 设备发送报警邮件 38
启用 FortiGate 设备发送入侵报警邮件功能 38
定制报警邮件消息 39
减少 NIDS 攻击日志和邮件消息的数量 39
自动减少消息 39

术语表 **41**

索引 43

概述

FortiGate NIDS 是一个实时的网络入侵探测器，它使用攻击定义库库检测和预防各种各样的可疑的网络数据流和基于网络的直接攻击。任何时候只要发生网络攻击，FortiGateNIDS 可以将事件记录进日志并给系统管理员发送报警邮件。

NIDS 模块

NIDS 由检测、预防和响应三个软件模块组成。关于 NIDS 模块的概述，请见：

- 使用 NIDS 检测模块检测入侵企图
- 使用 NIDS 预防模块预防入侵
- 使用 NIDS 响应模块管理消息

使用 NIDS 检测模块检测入侵企图

NIDS 检测模块可以检测各种各样的可疑网络通讯和基于网络的攻击。

FortiGateNIDS 检测模块的核心是攻击特征。特征是指示出系统可能正在受到攻击的传输数据的模板或者其他编码。从功能上看，特征类似于病毒定义，每个特征都用来检测特定类型的攻击。

FortiGate NIDS 使用了 1000D 多个攻击特征。为了保证您使用的是最新版本的攻击特征，您需要定期更新您的攻击签名文件。您可以将 FortiGate 设备配置为自动检查和下载包括了最新的特征的攻击定义的更新文件。或者您也可以手工下载攻击定义的更新文件。详细信息请见 *FortiGate 安装和配置指南*。

您也可以创建自己定义的特征。关于创建特征的详细信息请见 第 15 页 “ 创建用户定义的特征” 。创建了签名之后，您可以将它上载到 FortiGate 设备。只有专业 IT 人员才能创建用户定义的特征。

您可以启用 FortiGate NIDS 的攻击消息功能。FortiGate 设备可以配置为将攻击消息记录到攻击日志，并且可以将攻击消息编成报警邮件，最多发送到三个电子邮件地址。

使用 NIDS 预防模块预防入侵

FortiGate 设备能够作到的不仅仅是简单地检测攻击，它还可以预防攻击。NIDS 预防模块可以为您预防来自于破坏性的网络操作中的常规的 TCP、ICMP、UDP 和 IP 攻击。您可以启用 NIDS 预防模块以按照默认的临界值设定预防一系列攻击。当 NIDS 检测到一个与攻击定义匹配的入侵企图时，访问将被拒绝，或者数据包被丢弃从而防止网络遭到破坏。

NIDS 预防模块和 NIDS 检测模块一样，使用特征来检测攻击，并且它生成可以记录进日志或作为报警邮件发送的攻击消息。然而，尽管 NIDS 预防模块和 NIDS 检测模块十分相似，它们分别使用各自的特征并生成各自的消息。

当 FortiGate 设备接收到一个固件升级时，NIDS 预防模块中的特征列表将被更新。新的特征无法从 Fortinet 下载或者由用户创建。

使用 NIDS 响应模块管理消息

任何时候当检测或者预防一次攻击时，NIDS 响应模块生成一个可以记录攻击日志或生成最多可以发送到三个目的地址的电子邮件的消息。系统管理员可以利用这个信息及时地处理来自网络的威胁。

NIDS 检测和预防特性

NIDS 可以检测和预防以下类型的攻击：

- 拒绝服务（DoS）攻击
- 嗅探
- 权利提升
- NIDS 躲避

拒绝服务（DoS）攻击

拒绝服务攻击通过使网络连接过载、CPU 过载或者塞满硬盘来试图阻止对一个服务或者一台计算机的访问。攻击者并不试图获得任何信息，但是他干扰了对网络资源的访问。FortiGate NIDS 检测以下常规的 DoS 攻击：

- 数据包淹没，包括 Smurf 淹没 （Smurf 是最先使用这种攻击的一个程序的名称）、TCP 握手淹没、UDP 淹没和 ICMP 淹没。
- 非法格式的数据包，包括死亡之 ping(Ping of Death)，Chargen，死亡泪滴 （Tear drop）、land 和 WinNuke。

嗅探

嗅探攻击试图取得所要攻击或侵入的网络和电脑的信息。使用所得的信息，攻击者可以找到这个网络的弱点并加以攻击。FortiGateNIDS 可以检测以下类型的嗅探攻击：

- 指纹识别
- ping 扫描
- 端口扫描
- 缓冲区溢出，包括 SMTP、FTP 和 POP3
- 帐号扫描
- 操作系统识别

权利提升

权利提升攻击试图利用系统的特征或者缺陷对电脑或网络实行未经授权的访问。FortiGate NIDS 能检测以下类型的权利提升攻击：

- 暴力攻击
- CGI 脚本攻击、包括 Phf、EWS、info2www、TextCounter、GuestBook、Count.cgi、handler、webdist.cgi、files.pl、nph-test-cgi、nph-publish、任意 Form 和 Formmail。
- 网页服务器攻击。
- 网页浏览器攻击、包括 URL、HTTP、Java 脚本、Frames、Java 和 ActiveX。
- 简单邮件传送协议 （SMTP）（发送邮件 ） 攻击。
- IMAP/POP 攻击。
- 缓冲区溢出攻击。
- DNS 攻击，包括绑定和捕获。
- IP 欺骗。
- 特洛伊木马攻击，包括后门 （BackOrifice 2K）、 IniKiller、 Netbus、NetSpy、Priority、 Ripper、 Striker、和 SubSeven。

NIDS 躲避

随着攻击者变得越来越老练和狡猾，他们开发出一些新的技术来躲避 NIDS。FortiGate NIDS 可以识别出以下躲避 NIDS 的技术：

- 特征伪装
- 特征编码
- IP 碎片
- TCP/UDP 分解

关于本文档

本指南在以下章节中包含了一般配置步骤，基于 Web 的管理程序和 CLI 操作，以及配置举例：

- 检测攻击 描述例如如何配置一般的 NIDS 设置以及如何配置特征列表以使 FortiGate 设备可以检测攻击。
- 创建用户定义的特征 描述了您应当如何编写您自己定义的特征并将它添加到 FortiGate 设备。在添加了这些特征之后，它们可以用于检测攻击。
- 预防攻击描述了如何使用特征来预防攻击。
- 管理 NIDS 消息描述了如何配置 NIDS 以记录出现攻击时生成的日志消息并把它们发送到指定的电子邮件地址。
- 术语表定义了本文档中常用的术语。

2.50 版中的新增内容

以下为 2.50 版中新增加的特点。

NIDS 攻击 ID 编号

每个 NIDS 攻击具有一个 ID 编号，当检测到攻击时 NIDS 生成这个编号，它出现在报警邮件和攻击日志消息中。这样易于检索报警邮件或攻击日志消息中所涉及的攻击。请见 第 12 页 “ 查看特征列表” 。

特征组

在 NIDS 攻击模块中，攻击特征现在被分组排列。当您启用一个组时，这个组中的特征将被用于检测多种基于网络的攻击。当您禁用一个组时，这些特征将不被用于检测攻击。您不能启用或者禁用单独的一个特征。请见 第 7 页 “ 检测攻击” 。

入侵预防

在早期的 NIDS 版本中，NIDS 只能检测攻击，不能预防攻击。现在 NIDS 可以配置为预防来自破坏性的网络操作的常见 TCP、ICMP 和 IP 攻击。请见 第 25 页 “ 预防攻击” 。

新的 CLI 命令

在 2.50 版中命令行界面有了很大的改变。命令的语法变得更加易于使用和更加高效，很多命令名和关键词发生了变化，并且扩充了 CLI 帮助的内容。

文档约定

本指南使用以下约定来描述 CLI 命令的语法。

• 尖括号 <> 所围的内容为可替换的关键词

例如：

要执行 `restore config <文件名_字符串>`

您应当输入 `restore config myfile.bak`

`<xxx_字符串>` 表示一个 ASCII 字符串关键词。

`<xxx_整数>` 表示一个整数关键词。

`<xxx_ip>` 表示一个 IP 地址关键词。

• 竖线和波形括号 {|} 表示从波形括号中的内容中任选其一。

例如：

`set system opmode {nat | transparent}`

您可以输入 `set system opmode nat` 或 `set system opmode transparent`

• 方括号 [ ] 表示这个关键词是可选的

例如：

`get firewall ipmacbinding [dhcpipmac]`

您可以输入 `get firewall ipmacbinding` 或 `get firewall ipmacbinding dhcpipmac`

Fortinet 的文档

从 FortiGate 用户手册的以下各卷中可以找到关于 FortiGate 产品的对应信息：

- *第一卷：FortiGate 安装和配置指南*

  描述了 FortiGate 设备的安装和基本配置方法。还描述了如何使用 FortiGate 的防火墙策略去控制通过 FortiGate 设备的网络通讯，以及如何使用防火墙策略在通过 FortiGate 设备的网络通讯中对 HTTP、FTP 和电子邮件等内容应用防病毒保护、网页内容过滤和电子邮件过滤。
- *第二卷：FortiGate 虚拟专用网络 （VPN）指南*

  包含了在 FortiGate IPSec VPN 中使用认证、预置密钥和手工密钥加密的更加详细的信息。还包括了 Fortinet 远程 VPN 客户端配置的基本信息，FortiGate PPTP 和 L2TP VPN 配置的详细信息，以及 VPN 配置的例子。
- *第三卷：FortiGate 内容保护指南*

  描述了如何配置防病毒保护，网页内容过滤和电子邮件过滤，以保护通过 FortiGate 的内容。
- *第四卷：FortiGate NIDS 指南*

  描述了如何配置 FortiGate NIDS，以检测来自网络的攻击，并保护 FortiGate 不受其威胁。
- *第五卷：FortiGate 日志和消息参考指南*

  描述了如何配置 FortiGate 的日志和报警邮件。还包括了 FortiGate 日志消息的说明。
- *第六卷：FortiGate CLI 参考指南*

  描述了 FortiGate CLI，并且还包含了一个 FortiGate CLI 命令的说明。

FortiGate 在线帮助也包含了使用 FortiGate 基于 Web 的管理程序配置和管理您的 FortiGate 设备的操作步骤说明。

Fortinet 技术文档的注释

如果您在本文档或任何 Fortinet 技术文档中发现了错误或疏漏之处，欢迎您将有关信息发送到 techdoc@fortinet.com。

客户服务和技术支持

请访问我们的技术支持网站，以获取防病毒保护和网络攻击定义更新、固件更新、产品文档更新，技术支持信息，以及其他资源。网址：
http://support.fortinet.com。

您也可以到 http://support.fortinet.com 注册您的 FortiGate 防病毒防火墙或在任何时间登陆到该网站更改您的注册信息。

以下电子邮件信箱用于 Fortinet 电子邮件支持：

amer_support@fortinet.com	为美国、加拿大、墨西哥、拉丁美洲和南美地区的客户提供服务。
apac_support@fortinet.com	为日本、韩国、中国、中国香港、新加坡、马来西亚、以及其他所有亚洲国家和澳大利亚地区的客户提供服务。
eu_support@fortinet.com	为英国、斯堪的纳维亚半岛、欧洲大陆、非洲和中东地区的客户提供服务。

关于 Fortinet 电话支持的信息，请访问 http://support.fortinet.com。

当您需要我们的技术支持的时候，请您提供以下信息：

- 您的姓名
- 公司名称
- 位置
- 电子邮件地址
- 电话号码
- FortiGate 设备生产序列号
- FortiGate 型号
- FortiGate FortiOS 固件版本
- 您所遇到的问题的详细说明

检测攻击

NIDS 检测模块能够检测大量的可疑网络通讯和基于网络的攻击。

本章描述了如何配置常规的 NIDS 设置和 NIDS 检测模块特征列表。在常规 NIDS 设置中，您需要选择要监视基于网络的攻击的接口。您还需要决定是否启用校验和检验功能。校验和检验功能测试被监视的接口收到的数据包的完整性。

在特征列表中，您可以根据需要启用和禁用特征组。每个特征组包含了一定数量的特征，或者攻击定义。当起用一个特征组时，这个特征组中所包含的特征将被用于检测多种基于网络的攻击。当禁用一个组时，其中所包含的特征将不被用来检测攻击。

无论何时当 NIDS 检测到一个攻击时，它将生成一条 NIDS 响应消息。您可以将这个消息添加到攻击日志，还可以将它编写成电子邮件最多发送到三个目的地。有关的详细信息请见 第 37 页 “管理 NIDS 消息”。

本章叙述了以下内容：

• 特征组
• 特征举例
• 一般配置步骤
• NIDS 常规配置
• 选择一个特征组
• 更新攻击定义

特征组

FortiGate NIDS 使用了 1000D 多个攻击特征。这些特征被分组排列，每个组检测一种不同类型的攻击。NIDS 检测模块中的分组使用名称按照字母顺序排列。如果选择了查看一个特定的组的细节，您将看到它内部包含的特征的完整列表。

默认情况下，所有的组都被启用了，您可以选择禁用一个组使得这个组中的特征不再被用来检测攻击。无法启用或者禁用单独的一个特征。

您可以禁用一个特征组，以提高系统的性能，减少 NIDS 生成的日志消息和报警邮件的数量。例如，NIDS 检测到大量的网页服务器攻击。如果您没有提供对防火墙后边的网页服务器的访问，可以禁用所有的网页服务器攻击特征。

表 1：NIDS 特征分组

特征组名	说明
后门	检测使用后门技术穿过系统保护机制的攻击。

表 1: NIDS 特征分组 （续）

特征组名	说明
损伤	检测违反了系统安全策略的攻击。
ddos	检测分布式拒绝服务攻击。
dns	检测使用 DNS 的攻击。
dos	检测拒绝服务攻击。
权利提升	检测基于权利提升的攻击。
finger	检测使用 Finger 协议的攻击。
ftp	检测使用 FTP 协议的攻击。
icmp	检测使用 ICMP 协议的攻击。
imap	检测使用 IMAP 协议的攻击。
misc-traffic	检测使用混杂的有害通讯技术的攻击。
netbios	检测使用 NETBIOS 协议的攻击。
pop2	检测使用 POP2 协议的攻击。
pop3	检测使用 POP3 协议的攻击。
rlogin	检测用户远程登录以获取计算机网络中的信息的攻击。
rpc	检测使用 RPC 协议的攻击。
scan	检测不同类型的端口扫描和相关的嗅探攻击。
shellcode	检测包含了特种操作系统的命令解释器代码的攻击。
smtp	检测使用 SMTP 协议的攻击
snmp	检测使用 SNMP 协议的攻击。
sql	检测利用 SQL 漏洞的攻击。如果 FortiGate 设备保护的网页服务器或者其他应用程序运行 MS-SQL 或者 MS-SQL/SMB，则启用此特征组。
telnet	检测使用 Telnet 协议的攻击。
tftp	检测使用 TFTP 协议的攻击。
web-apache web-attacks web-cgi web-client web-coldfusion web-domino web-frontpage web-iis web-misc web-netscape web-php web-tomcat	检测基于网页的攻击，包括利用 CGI， ColdFusion， FrontPage， IIS，客户端和 PHP 的漏洞进行的攻击。
端口扫描	检测对一个主机的一定范围内的服务端口地址发送客户请求以找出活动的端口并利用这个服务的漏洞进行的攻击。
http 解码	检测使用 HTTP 协议的攻击。
backorifice	检测使用 Back Orifice 木马来监视或篡改微软 Windows 操作系统的攻击。
rpc 解码	检测包含了 RPC 记录的攻击。
tcp 重组	检测使用 TCP 协议的攻击。
IP 碎片	检测使用破碎的 IP 数据包进行的攻击。

表 1: NIDS 特征分组 （续）

特征组名	说明
包格式	检测使用非标准头的包或者超长包进行的攻击。
用户定义	检测新的使用用户自行定义的特征的攻击。请见 第 15 页 “ 创建用户定义的特征” 。

特征举例

在特征组中包含了独立的特征。如果您查看一个给定的组，您将看到这个组包含的特征的完整列表。每个特征都有一个 ID 编号，名称和修订版本编号。

以下几个表格中包含了一些特征的例子：

- 表 2 列出了可以用于检测拒绝服务攻击 （DoS）的特征。
- 表 3 列出了可以用来检测嗅探攻击的特征。
- 表 4 列出了可以用来检测漏洞攻击的特征。

注意：在列表中包含的值仅为举例。要查看特征组和组中包含的特征的完整的当前列表，请查看一个运转中的 FortiGate 设备。

表 2: DoS 特征举例

攻击类型	特征组名称	特征 ID 举例	特征规则举例
拒绝服务	ddos	17563649	DDOS TFN 探测
	dos	917505	DOS 晃动攻击
	混合通讯	101974020	混合。通讯源端口为 20 到小于 1024。
	ip 碎片	7405573	重复的第一段。
	包格式	7602271	UDP 包头被截断
	rpc 解码	6946820	不完整的 RPC 段

表 3: 嗅探特征举例

攻击类型	特征组名称	特征 ID 举例	特征规则举例
嗅探	finger	101711873	Finger 溢出 (>128) 企图
	icmp	17956865	ICMP ISS Pinger
	rlogin	102236167	rlogin root
	rpc	286851134	RPC 端口映射请求状态
	scan	102367236	扫描代理的企图
	shellcode	1769486	linux 命令解释器命令代码
	portscan	6553602	(spp_ 端口扫描 ） 端口扫描状态
	tcpassembly	7274504	秘密活动 （FIN 扫描 ） 检测

表 4：漏洞攻击特征

攻击类型	特征组名称	特征 ID 举例	特征规则举例
漏洞攻击	后门	101318672	Back door subseven 22
	危害	101384193	Successful gobbles ssh 权利提升 (GOBBLE)
	dns	286064641	利用 Solaris tsig 的数据包
	权利提升	101646338	利用 ssh CRC32 溢出 /bin/sh
	ftp	101777411	带有？的 FTP 命令 STAT
	netbios	102039554	NETBIOS nimda .eml
	rpc	102301722	RPC snmpXdmi 溢出企图
	smtp	102498305	SMTP sendmail 8.6.9 版权利提升
	sql	102629377	MS-SQL/SMB sp_start_job - 程序执行
	telnet	102694920	Telnet 错误登录
	tftp	287309825	TFTP GET Admin.dll
	web-attacks	102891521	试图利用网页攻击 ps 命令
	web-cgi	102957107	Web-CGI 对 bnbform.cgi 访问
	web-coldfusion	103088129	Web-ColdFusion cfcache.map 访问
	web-frontpage	103219201	Web-FrontPage rad 溢出企图
	web-iis	103284737	Web-IIS 对 repost.asp 文件的访问
	web-misc	103350273	Web-Misc. 企图穿过站点脚本的企图
	httpdecode	6684678	(spp_http_decode) 非法 URL 十六进制编码
	backorifice	6881281	(spo_bo) Back Orifice 通讯检测

一般配置步骤

要配置 NIDS 检测网络攻击的功能，您必须完成两个基本的步骤。首先您必须配置常规 NIDS 设置。然后您必须查看特征列表，决定启用那个组来检测攻击。默认情况下，所有的特征组都被启用了。

按以下步骤配置 NIDS 以检测攻击：

1 配置常规 NIDS 设置。在选择了您希望 NIDS 监视的接口之后，您可以选择是否启用在这些接口上的校验和检验。请见 第 11 页 “ NIDS 常规配置” 。

2 选择您希望 NIDS 用来检测基于网络的攻击的特征组。请见 第 12 页 “ 选择一个特征组” 。

3 您可以选择将 FortiGate 设备配置为自动检查新版本的攻击定义。请见 第 14 页 “ 更新攻击定义” 。

NIDS 常规配置

要启用 FortiGate NIDS，您必须至少选择一个要监视来自网络的攻击的接口。要禁用 FortiGate NIDS，您必须取消对任何一个接口的选定。

注意：最多可以监视四个接口 (FortiGate-50 只能监视一个接口）。

选择要监视的网络接口

1 进入 NIDS > **检测** > **常规**。

2 选择要检测网络攻击的网络接口。

您可以选择一个或多个网络接口。

3 单击**应用**以保存您所做的修改。

使用 CLI：

```
set nids detection interface <名称_字符串> status enable
```

禁用 NIDS

1 进入 NIDS > **检测** > **常规**。

2 取消对所有监视的接口的选定。

3 单击 **应用** 以保存您所做的修改。

使用 CLI：

```
set nids detection interface <名称_字符串> status disable
```

配置校验和检验

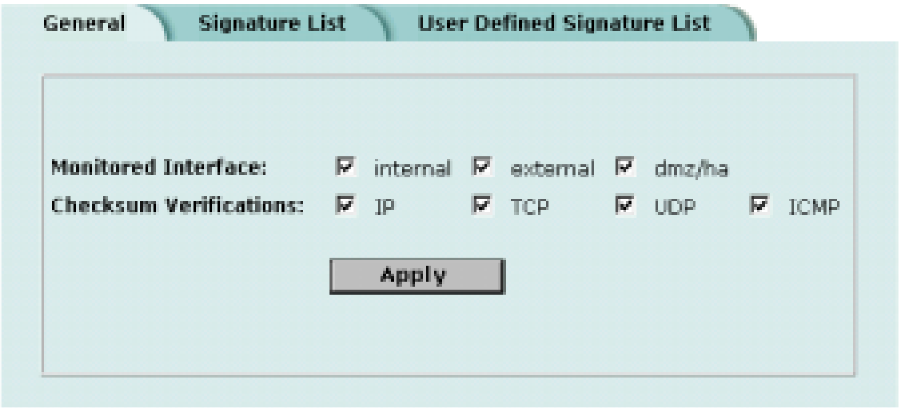
校验和验证测试通过 FortiGate 的文件，确保他们在传送过程中没有被篡改。NIDS 可以在 IP、TCP、UDP 和 ICMP 数据流上进行校验和检查。如果要进行最大限度的检查，您可以启用所有类型数据流的校验和检查。然而，如果 FortiGate 不需要进行校验和验证，您可以关掉部分或者全部类型的数据流的校验和验证，这样可以提高网络传输性能。如果您的 FortiGate 是安装在一个同样进行校验和验证的路由器后面，您就没有必要再进行校验和验证。

1 进入 NIDS > **检测** > **常规**。

2 选中要验证校验和的数据流类型。

3 单击 **应用** 以保存您所做的修改。

图 1: FortiGate-300 设备的 NIDS 检测配置举例



使用 CLI：

```
set nids detection checksum {none | ip,tcp,udp,icmp}
```

选择一个特征组

FortiGate NIDS 检测模块使用的特征组编入了 1000 多个特征。默认情况下，所有的组都被启用了。

为了优化系统性能，您可以禁用一些组。如果您禁用了一个组，FortiGate NIDS 将不再使用这个组中包含的特征进行入侵企图的检测。您不能启用或者禁用组中的单独一个特征。

查看特征列表

按如下操作显示当前 NIDS 特征组列表和某个特征组的成员：

1 进入 NIDS > **检测** > **特征列表**。

2　查看列表中的特征组的名称和状态。

NIDS 使用列表中所有选中了启用列的特征组进行攻击检测。

注意：用户定义的特征组是特征列表中的最后一项。请见 第 15 页 “创建用户定义的特征”。

3　选择查看细节可以显示一个特征组的特征成员。

特征组成员列表显示了每一个组成员的攻击 ID，规则名称，和修订版本号。

图 2:　特征组成员列表举例

exploit		
ID	**Rule Name**	**Revision**
101646337	gobbles SSH exploit attempt	16
101646338	ssh CRC32 overflow /bin/sh	16
101646339	ssh CRC32 overflow NOOP	16
101646340	ssh CRC32 overflow	16
101646341	x86 linux samba overflow	16
101646342	Solaris x86 nlps overflow attempt	16
101646343	nlps x86 solaris overflow	16
101646344	LPRng overflow	16
101646345	redhat 7.0 lprd overflow	16

启用和禁用 NIDS 攻击特征

默认情况下，所有的特征组都被启用了。禁用不必要的 NIDS 攻击特征组可以提高系统的性能，减少 FortiGate NIDS 生成的日志消息的数量和报警邮件的数量。例如，NIDS 检测到了大量的网页服务器攻击。如果您没有在您的防火墙后的网络中提供网页服务，您可以禁用全部网页服务器攻击特征。

注意：为了保护您的 NIDS 特征设置，Fortinet 建议您在更新固件之前备份 NIDS 攻击特征设置。您可以在完成更新之后恢复保存了的配置。

按以下步骤禁用 NIDS 攻击特征：

1　进入 NIDS > **检测 > 特征列表。**

2　卷动特征列表，找到要禁用的特征。

攻击日志和报警邮件中的特征名称和 ID 号与攻击列表中的相对应。您可以很容易地通过 ID 号在特征列表中找到特定的特征定义。

3　取消对特征旁边的活动选项的选中。

4　单击确定。

5　对于每一个您要禁用的 NIDS 攻击特征组重复步骤 2 和步骤 4。

单击全部选中可以启用特征列表中的全部的 NIDS 攻击特征组。

单击全部取消可以取消对特征列表中的全部的 NIDS 攻击特征组的选中。

注意：攻击消息可以记录到攻击日志和用电子邮件发送给系统管理员。请见 第 37 页 “管理 NIDS 消息”。

使用 CLI：

```
set nids rule <组名_字符串> status {enable | disable}
```

更新攻击定义

您可以将 FortiGate 设备配置为自动检查新版本的攻击定义。如果 FortiGate 发现了新版本的攻击定义，它将自动下载和安装新版本的攻击定义。您也可以手工更新攻击定义。

关于攻击定义更新的配置的详细信息，请见 *FortiGate 安装和配置指南。*

注意：更新攻击定义只更新攻击检测特征，不更新攻击预防特征。

创建用户定义的特征

特征是用来判断系统可能正在受到攻击的依据，它可以是传输数据模版或者其他编码。

您可以将用户自行定义的特征规则添加到 FortiGate NIDS 以检测没有包含在当前攻击定义文件中的攻击类型。

您可以使用本章中所描述的语法在一个文本文件中创建用户自定义的特征规则。然后将这个文本文件上载到 FortiGate 设备中。FortiGate 设备会为文件中的每个规则分配一个唯一的 ID，并且将它添加到特征组列表中的用户自定义组中。

一旦您创建并上载了用户定义的特征列表，您可以从 FortiGate 设备中将用户定义特征列表下载并保存到管理员电脑中的一个备份文件中。然后您可以在这个用户定义特征列表中编辑或者添加新的特征规则，还可以再次将它上载到 FortiGate 设备。

注意：用户定义的特征是一项高级功能，只有熟悉程序的概念和网络入侵检测系统的 IT 专业人事才能创建和添加用户自定义特征。

本章描述了如下内容：

- 创建用户自定义的特征
- 常规配置步骤
- 用户定义特征的语法
- 管理用户定义的特征

创建用户自定义的特征

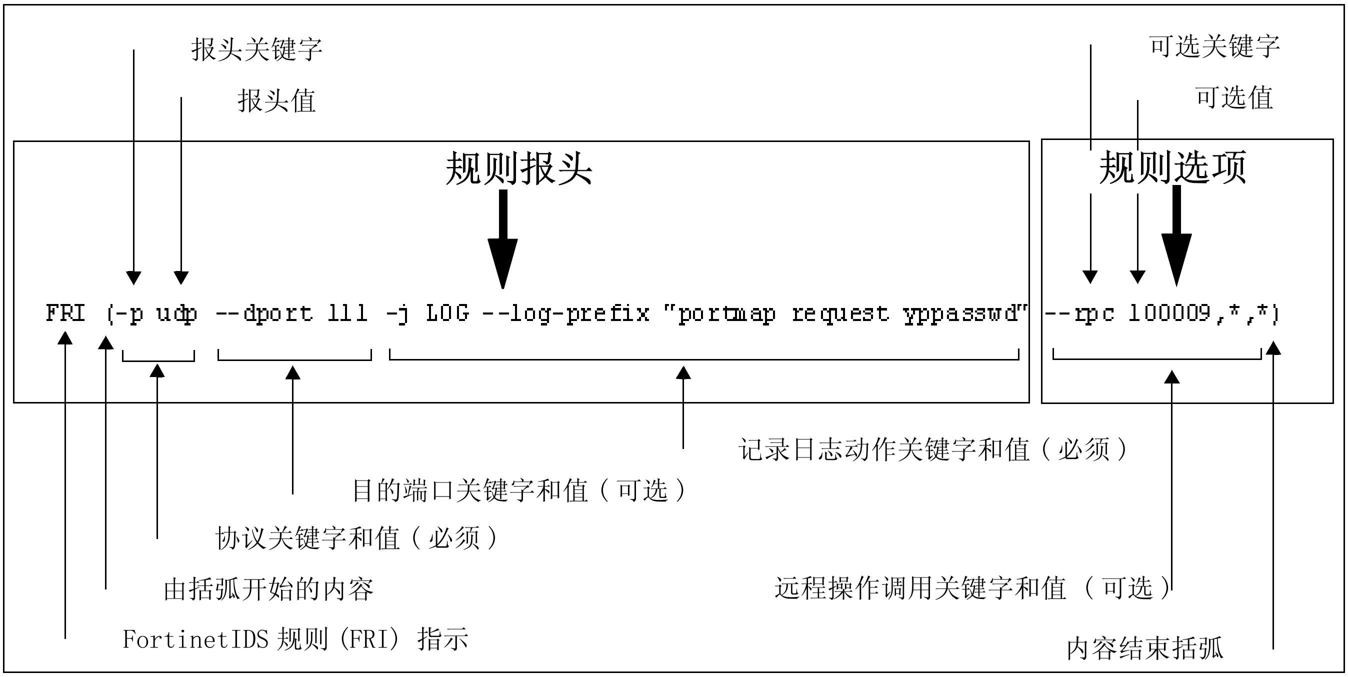
您可以使用简单，轻巧的规则描述语言来创建用户自定义的特征。

使用规则描述语言时需要牢记以下条原则：

- 用户自定义的特征本身可以看作一条规则。
- 每个特征必须在单独的一行中输入。Fortinet 规则分析器不知道如何读取写在多行的规则。
- 一个特征包括两个逻辑段，规则报头和规则选项。规则报头包含一个动作 （永远是将威胁记录到日志和发送一条报警消息）和基本的匹配元素。基本的匹配元素包括协议和可选的源 IP 地址和目的 IP 地址，以及端口号。规则选项段包括一些附加的内容，大多数用来检测数据包中的威胁的匹配元素。
- 组成一条特征的所有元素对于要执行的威胁的检测和动作 （将威胁记录日志并发送一条警报）都必须为真。
- 单一的特征中的元素组成了一个逻辑与表达式。特征列表中的所有特征的集合组成了一个逻辑或表达式。

图 3 用户定义的特征中的各种元素图示。

图 3:　　用户自定义的特征举例



用户定义特征提示

- 每个特征必须由 FRI （Fortinet IDS 规则）指示符开始。
- 特征的内容 （FRI 之后的部分）必须用括号括起来。
- 一个单独的连词符 “-” 引入一个关键字字符 （例如，-p），一个双连词符 “--” 引入一个关键词全称 （例如，--log-prefix）。
- 空格用于分隔特征的元素 （关键字和值的组合）。
- 逗号用于分隔可以在任何组合中输入且必须用逗号分隔的可选项。
- 双引号包括的为字符串。双引号内包括的字符串可以包含空格。
- 星号 “*” 可以匹配任何字符，任意多个字符。问号匹配单一字符。一个惊叹号反转匹配的结果 （匹配除了指定值外的所有值）。
- 每个特征最少要包括两个元素：协议和日志动作。其他的所有元素都是可选的。例如：
  `FRI (-p <协议_字符串> -j LOG --log-prefix “前缀_字符串”)`
- 通讯的方向是从源到目的地址，除非您在规则报头段包含了 --bi-dir 选项。

常规配置步骤

按如下步骤配置用户定义的特征：

1. 使用在本指南中描述的语法创建一个包含了用户定义的特征的文本文件，请见 第 17 页 “ 用户定义特征的语法” 。
2. 将用户定义特征文本文件从管理员电脑上载到 FortiGate 设备。请见 第 24 页 “ 管理用户定义的特征” 。

用户定义特征的语法

本节阐述了用于创建用户定义特征的语法。本节分为以下三个部分：

- 语法约定阐述了用于本章的语法约定。
- 完整的特征语法提供了一个完整的不带任何描述的语法例子。
- 特征语法的细节提供了每个语法元素的详细说明。

语法约定

本指南使用以下约定来描述特征语法：

- 尖括号 <> 表示可变关键字或值。
- 竖线和波型括号 {|} 分隔二选一的、互斥的关键字或值。
- 方括号 [] 表示关键字或值是可选的。

完整的特征语法

以下语法包含了用于创建用户定义特征的所有可用的元素。

```
   FRI
(
-p <协议_字符串>
[-s <源-ip_范围/网络掩码>]
[-d <目的-ip_范围/网络掩码>]
[--sport <开始-端口_整数:结束-端口_整数>]
[--dport <开始-端口_整数:结束-端口_整数>]
[--bi-dir]
-j LOG --log-prefix “前缀_字符串”
[--rev <版本_整数>]
[--reference <系统_字符串><id_字符串>]
[--content “内容_字符串”]
[--offset <偏移量_整数>]
[--depth <深度_整数>]
[--uri “URI_字符串”]
[--nc --regex]
[--sameip]
[--fragment <比特值_字符串>
[-ttl <ttl_整数>]
[-tos <tos_整数> -id <id_整数>]
[-ip-option <ipoption_字符串>]
[-dsize [<>]<大小_整数>[<><大小_整数>]]
[--tcp-flags <标志_字符串>[,<掩码_字符串>]]
[--tcp-seq <次序_整数>]
[--tcp-ack <应答_整数>]
[--tcp-session <会话_整数>]
[--rpc <应用程序_整数> [,<进程_整数> | *]
[,<版本_整数> | *]]
[--icmp-type <类型_整数>]
[--icmp-code <代码_整数> --icmp-id <id_整数>]
[--icmp-seq <seq_整数>]
)
```

特征语法的细节

以下部分包含了用于创建用户定义特征的全部的可用的元素的详细说明。此表分为两部分：规则报头元素和规则选项元素。

规则报头元素

除了基本的匹配元素（协议和可选的源 IP 地址和目的 IP 地址和端口）之外，规则报头还包含一个动作元素，它定义了如果 Fortinet 规则分析器截获了一个匹配特征规则的数据包时的动作。

- 第 20 页 表 5 描述了基本匹配元素的语法。只有协议元素是必须的。
- 第 21 页 表 6 描述了动作元素的语法。Fortinet 规则分析器只能执行一个动作，即将威胁记录到日志并发送一封报警邮件消息。除了启用这个动作之外，您必须指定一个消息前缀。您还可以选择是否添加一个规则修订版本号和一个外部攻击分类系统 ID 的引用。

规则选项元素

规则选项元素决定了 Fortinet 规则分析器需要检查数据包的哪一部分以判断是否存在攻击。这些元素是可选的；任何规则都不是必须有这些元素，但是这些元素能够提供对数据包的检测的更加灵活的控制功能。

- 第 21 页 表 7 描述了内容模版元素的语法。它指定了 Fortinet 规则分析器如何在文本、二进制数据或两者中查找基于内容模板的匹配内容。您可以使用内容模板选项控制以下内容：
  - 对数据包的特定位置进行匹配的偏移量和深度值的限制
  - URI 模板匹配
  - 区分大小写
  - 通配符匹配
  - 源地址和目的地址比对
- 第 22 页 表 8 描述了 IP 元素的语法。它指定了 Fortinet 规则分析器如何查找匹配的 IP 头和有效载荷特征。
- 第 23 页 表 9 描述了 TCP 元素的语法。它指定了 Fortinet 规则分析器如何查找匹配的 TCP 标志、序列和会话信息。
- 第 23 页 表 10 描述了 ICMP 元素的语法。它指定了 Fortinet 规则分析器如何查找匹配的 ICMP 域信息。

表 5：协议，源地址和目的地址 （规则报头）

关键字	说明
`-p` < 协议 _ 字符串 >	这是一个必须的条目。 匹配指定的由逗号分隔的协议或协议族，例如： `-p tcp,udp,icmp,ip`。
`-s` <源-`ip_` 范围 / 网络掩码 >	根据源地址或地址范围匹配数据包。 • IP 地址可以是单独的一个地址或者一个地址范围。例如 `192.168.1.1` 匹配单独的IP地址, `192.168.1.0`匹配 192.168.1.0 子网中的地址 , 而 `192.168.1.1-192.168.1.10` 匹配这一地址范围内的地址。 • 网络掩码可以是`/255.`*`xxx.xxx.xxx`* 格式或者 CIDR 格式/*yy*。*yy* 是网络掩码的网络一侧的数字，例如 192.168.1.1/32。 使用 ! 可以反转匹配。例如 `-s !192.22.33.0/24` 匹配所有源地址不在 192.22.33.0 子网的数据包。如果 -s 选项没有被使用，默认情况下不匹配任何源地址。
`-d` < 目的 -`ip_` 范围 / 网络掩码 >	根据目的地址或地址范围匹配数据包。 • IP 地址可以是单独的一个地址或者一个地址范围。例如：`192.168.1.1` 匹配单独的IP地址, `192.168.1.0`匹配 192.168.1.0 子网中的地址 , 而 `192.168.1.1-192.168.1.10` 匹配这一地址范围内的地址。 • 网络掩码可以是`/255.`*`xxx.xxx.xxx`* 格式或者 CIDR 格式/*yy*。*yy* 是网络掩码的网络一侧的数字，例如 192.168.1.1/32。 使用 ! 可以反转匹配。例如 `-s !192.22.33.0/24` 匹配所有源地址不在 192.22.33.0 子网的数据包。如果 -s 选项没有被使用，默认情况下不匹配任何源地址。
`--sport` <开始-端口_整数 : 结束 - 端口 _ 整数 >	根据源端口或端口范围匹配 TCP 或 UDP 数据包。端口号可以是单独的一个端口或者一个端口范围。例如，22 匹配 22 端口，22:80 匹配 22 和 80 端口。在端口范围设置中，如果省略了第一个端口，则假定为端口 0。例如，--sport :80 可以匹配从 0 到 80 的端口。如果省略了最后一个端口，则假设为端口 65535，例如 --sport 22: 匹配从 22 到 65535 端口。 使用 ! 可以反转匹配。例如 --sport !22 匹配所有除了 22 之外的所有端口，--sport!22:80 可以匹配除了从 22 到 80 之间的任何端口。如果选项没有被使用，默认情况下匹配任何源地址。
`--dport` <开始-端口_整数 : 结束 - 端口 _ 整数 >	根据目的端口或端口范围匹配 TCP 或 UDP 数据包。端口号可以是单独的一个端口或者一个端口范围。例如，22 匹配 22 端口，22:80 匹配 22 和 80 端口。在端口范围设置中，如果省略了第一个端口，则假定为端口 0。例如，--sport :80 可以匹配从 0 到 80 的端口。如果省略了最后一个端口，则假设为端口 65535，例如 --sport 22: 匹配从 22 到 65535 端口。 使用 ! 可以反转匹配。例如 --sport !22 匹配所有除了 22 之外的所有端口，--sport!22:80 可以匹配除了从 22 到 80 之间的任何端口。如果选项没有被使用，默认情况下匹配任何源地址。
`--bi-dir`	匹配双向的地址和端口对的通讯。使用这一选项可以同时分析会话的两侧，例如 telnet 或者 pop3 会话。

表 6：日志动作元素（规则报头）

关键字	说明
-j LOG	为这条规则在 IDS 日志中添加消息。 这一元素必须出现在紧随着协议、源和目的地址定义之后，在日志前缀字符串之前。例如： -p udp --dport 10080:10081 -j LOG “INPUT packets” 关于进一步的详细信息请见 *FortiGate 日志配置和参考指南*中的 IDS 日志消息。
--log-prefix “prefix_str”	为这条规则对应的 NIDS 报警邮件消息和 IDS 日志消息添加一个前缀。
--rev < 版本 _ 整数 >	在规则中识别这条规则的修订版本。规则的修订版本跟规则的 ID 一起可以替换和更新特征和有关特征的具体说明。
--reference < 系统 _ 字符串 ><id_ 字符串 >	包含了一个在外部攻击识别系统中的规则 ID 的引用。例如， 在这条规则中引用在 www.securityfocus.com/bid/ 的 Bugtraq。

表 7：内容元素（规则选项）

关键字	说明
--content “ 内容 _ 字符串 ”	在数据包的有效部分中搜索完全匹配与模板的内容。内容字符串可以包含混合的二进制数据（以字节编码形式出现，并用分隔符“|”围起来的内容）和字符。例如： --content “|90C8 C0FF FFFF|/bin/sh” 不要在内容字符串中使用以下字符：;\“” 使用惊叹号“！”可以匹配不包含内容字符串中指定的内容的数据包。例如，!″GET″ 匹配所有不包含 GET 单词的数据包。 使用 --nc 可以设置为不考虑大小写，如果您使用了通配符则需要加上 --regex 。
--offset < 偏移量 _ 整数 >	使用以字节为单位的数字指定使用内容模板对数据包的有效内容进行匹配时，搜索启始位置从数据包的有效内容的起点的偏移量。例如，输入 3 可以从第四个字节处开始用内容模板进行匹配。
--depth < 深度 _ 整数 >	指定进行模板匹配的最大深度。这一选项限制了模板匹配功能使用给定的内容字符串进行搜索的范围。例如，输入 20 可以将搜索限制在 20 个字节之内。
--uri “URI_ 字符串 ”	在数据包的统一资源指示（URI）中使用内容模板搜索。这一选项仅在请求的 URI 部分中进行搜索，避免了来自服务器数据文件的虚假警报。 使用 --nc 可以设置为不考虑大小写，如果您使用了通配符则需要加上 --regex 。 使用惊叹号“！”可以反转匹配，使得 Fortinet 规则分析器匹配任何不包含指定内容的 URI 字符串。
--nc	在匹配功能处理内容字符串和 / 或 URI 字符串的时候不考虑大写和小写字符的区别。
--regex	在内容字符串和 / 或 URI 字符串中使用一个通配符模板进行匹配。如果您使用了 --regex，Fortinet 规则分析器使用星号“*”匹配内容字符串或 URI 字符串中的任意数量的任何字符，使用问号“？”匹配任何单一的字符。
--sameip	匹配源 / 目的 IP 地址相同的数据包。在规则消息前缀中这一选项可以写成“SRC IP = DST IP”。

表 8： IP 元素（规则选项）

关键字	说明
--fragment < 比特值 _ 字符串 >	匹配 IP 头中的片段和保留位： • M: 更多位片段 • R: 保留位 • D: 不分隔位 在位值字符串中列出一个或多个位 （不使用逗号）。例如， --fragment MR 匹配位片段和保留位。 使用惊叹号 “！” 可以匹配没有置位的位。例如， --fragment !R 匹配没有置位的保留位。
-ttl <ttl_ 整数 >	匹配 IP 头中的有效期 （TTL）的值。这一选项用于检测企图使用 traceroute 的数据包。
-tos <tos_ 整数 >	匹配 IP 头中的服务类型 （TOS）域。
-id <id_ 整数 >	匹配 IP 头中的片段 ID 域的值。有些黑客工具会将这个域置位；例如，很多黑客常使用 31337 这个值。
-ip-option <ip 选项 _ 字符串 >	匹配 IP 选项域： • rr: 记录路由 • eol: 列表结尾 • nop: 无选项 • ts: 时间标记 • sec: IP 安全 • lsrr: 松散源路由 • ssrr: 严格源路由 • satid: 流识别符 例如，-ip-option lsrr 匹配 IP 选项域设置为 lsrr 的数据包。松散和严格源路由选项在互联网应用程序中并不常用，所以 NIDS 经常监听这些选项上的攻击。每个规则仅指定一个选项。
-dsize [<|>]< 大小 _ 整数 > [<|>]< 大小 _ 整数 >	匹配有效载荷的尺寸符合某一数值或在某一数值范围内的 IP 数据包。使用大于号和小于号来表示范围。例如，如果某个服务有一个指定范围的缓冲区，可以通过设定这个选项来监视缓冲区溢出攻击。这一选项测试缓冲区溢出的速度比有效载荷内容检查要快。 大于号和小于号操作符是可选的。例如，dsize >400<500 返回所有的有效载荷部分在 400 到 500 字节之间的数据包。 对流重建的数据包的匹配结果永远为假。

表 9: TCP 元素 （规则选项）

关键字	说明
--tcp-flags <标志_字符串>[,<掩码_字符串>]	匹配数据包中的 TCP 标志设置。 • F: FIN • S: SYN • R: RST • P: PSH • A: ACK • U: URG) • 2: reserved bit 2 • 1: reserved bit 1 • 0: no TCP flags set 您可以使用以下逻辑运算符： • + 同时匹配指定的标志和其他任意标志。 • * 匹配任意一个指定的标志。 • ! 在指定标志没有置位的时候才匹配。 例如： • --tcp-flags SA 如果 SYN 和 ACK 标志置位时匹配。 • --tcp-flags A+ 如果 ACK 和任何其他标志置位时匹配。 • --tcp-flags !SA 如果 S 和 A 标志没有置位时匹配。 您可以指定一个可选标志，以指定规则检测会话初始化数据包，比如直接拥塞指示 (ECN) 包 (保留位的第一、二比特置位的 SYN 数据包）。例如，如果您希望匹配 SYN 数据包，不管它的保留位的值是多少，可以让 Fortinet 规则分析器检查 s,12 标志的值。
--tcp-seq <序列_整数>	匹配 TCP 静态序列域的值。
--tcp-ack <应答_整数>	匹配 TCP 头应答域的值。用来检测 NMAP TCP ping，它将此域设置为零并发送一个带有 TCP ACK 标志的数据包以判断一台网络中的主机是否在活动中。
--rpc <应用程序_整数> [,<进程_整数> | *] [,<版本_整数> | *]	检查远程过程调用 （RPC）请求和匹配应用程序、过程和程序的版本。可以同时使用通配符、过程和版本号。例如，rpc 100000,*,3。

表 10: ICMP 元素 (规则选项)

关键字	说明
--icmp-type <类型_整数>	匹配 ICMP 类型域的值。RFC792 指定了数值，有些已经废弃了。您可以范围外的值以检测有些 DoS 和淹没攻击使用的合法范围外的值。
--icmp-code <编码_整数>	匹配 ICMP 编码域的值，类似于类型域的值。您可以设置一个范围外的值以检测可疑的通讯。
--icmp-id <id_整数>	匹配 ICMP ECHO 数据包的 ICMP ID，有些隐蔽通道的程序在通讯时使用静态 ICMP 域。
--icmp-seq <seq_整数>	匹配 ICMP ECHO 包中的 ICMP 序列域的值。有些隐蔽通道的程序在通讯时使用静态 ICMP 域。

管理用户定义的特征

创建或编辑完用户定义特征列表后，您可以将它们上载到 FortiGate 设备。用户定义特征列表的功能类似于 NIDS 中的一个特征组。如同其他任何一个特征组一样，它可以被启用和禁用。

您还可以从 FortiGate 设备中下载用户定义特征列表。在特征列表中编辑或添加了更多的特征之后，您可以将它再次上载到 FortiGate 设备中。

上载用户定义特征列表

按以下步骤将用户定义特征列表从管理员电脑上载到 FortiGate 设备：

1 进入 NIDS > **检测** > **用户定义特征列表。**

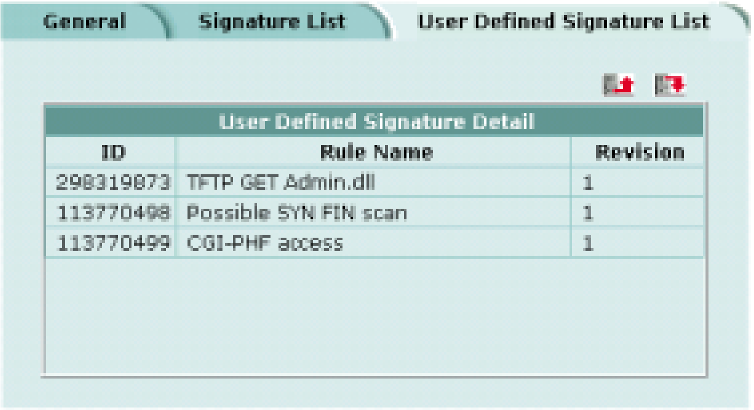
2 单击上载 。

3 输入用户定义特征列表的文本文件的路径和文件名，或者单击浏览以定位文件。

4 单击确定以将用户定义特征列表的文本文件上载到 FortiGate 设备。

5 单击返回以显示上载的用户定义特征列表。

图 4:　　用户定义特征列表举例



使用 CLI:

```
execute restore nidsuserdefsig <名称_字符串> <tftp_ip>
```

下载用户定义特征列表

按以下步骤下载用户定义特征列表：

1 进入 NIDS > **检测** > **用户定义特征列表。**

2 单击下载 。

FortiGate 将用户定义特征列表下载到管理员电脑并保存为文本文件。您可以指定下载的文本文件名和保存的位置。

3 编辑完特征列表后，您可以再次将它上载，请见 第 24 页 “管理用户定义的特征”。

使用 CLI:

```
execute backup nidsuserdefsig <名称_字符串> <tftp_ip>
```

预防攻击

NIDS 预防模块可以为您抵御来自破坏性的网络操作的各种常见的 TCP、ICMP、UDP 和 IP 攻击。您可以启用这个 NIDS 预防模块以使用一组默认的临界值去预防默认设置中的攻击。您还可以单独启用和设置某个攻击特征的临界值。

类似于 NIDS 检测模块，NIDS 预防模块使用特征来检测攻击，并且它还生成可以记录到日志和作为电子邮件发送的攻击消息。然而，尽管 NIDS 预防模块和 NIDS 检测模块运行方式十分相似，它们却使用各自的特征并生成各自的消息。

当 FortiGate 设备接收到一个新版本的软件的时候，它更新 NIDS 预防模块的特征列表。不能从 Fortinet 下载新特征或者由用户自己创建。

本章叙述了如下内容：

- 一般配置步骤
- 启用 NIDS 攻击预防
- 启用 NIDS 预防特征
- 配置特征临界值
- 配置 syn 淹没特征值
- 举例：NIDS 配置

一般配置步骤

您至少要先启动 NIDS 预防模块。然后您可以决定启用和禁用哪些特征。还可以修改某些特征的临界值。

按如下步骤配置 FortiGate 设备预防网络攻击的功能：

1. 启用 NIDS 预防模块。
   默认情况下这个模块是禁用的，请见 第 26 页 “ 启用 NIDS 攻击预防” 。
2. 启用您希望用来保护您的网络，抵御特定类型的攻击的 NIDS 保护特征。
   某些特征在默认配置中就已经启用了。其它的必须手工选定。请见 第 27 页 “ 启用 NIDS 预防特征” 。
3. 可以选择是否配置特征的临界值设置。
   当某个临界值被超越时，NIDS 预防模块将阻塞您的网络上的对应的攻击。请见 第 31 页 “ 配置特征临界值” 。
4. 可以选择配置淹没特征的临界值。
   除了临界值之外，淹没特征还有其他您可以配置的值设置，请见 第 32 页 “ 配置 syn 淹没特征值” 。

注意：在 FortiGate 设备重新启动后，NIDS 预防模块和淹没预防功能都将被自动禁用。

启用 NIDS 攻击预防

NIDS 预防模块在默认情况下是禁用的。当您配置一个新的 FortiGate 设备，或者您重新启动一个 FortiGate 设备时，必须手工启动它。

按如下步骤启动 NIDS 攻击预防：

1. 进入 **NIDS > 预防**。
2. 单击左上角的启用。

使用 CLI:

```
set nids prevention status enable
```

启用 NIDS 预防特征

NIDS 预防模块包括用来保护您的网络免受攻击的一些特征。有些特征在默认情况下就已经启用了，其它的必须手工启用。关于 NIDS 预防特征及其说明的完整列表请见 第 28 页 “ NIDS 预防特征说明” 。

除了启用和禁用特征之外，您还可以修改它们。对于某些特征，您还可以修改他们的临界值。请见 第 31 页 “ 配置特征临界值” 。对于 SYN 淹没攻击预防，您可以修改临界值，队列长度和超时设置。请见 第 32 页 “ 配置 syn 淹没特征值” 。

启用 NIDS 预防特征

1 进入 NIDS > 预防。

2 选中每个您要启用的特征旁边的启用列的核选框。

3 单击全部选中 可以启用 NIDS 预防特征列表中的全部特征。

4 单击全部取消 可以禁用 NIDS 预防特征列表中的全部特征。

5 单击设置为默认值 可以只启用默认的 NIDS 预防特征并将临界值恢复到默认值。

图 5: NIDS 预防特征列表举例

Prevention

☑ Enable Prevention

Signature Abbreviation	Summary	Protocal	Enable	Modify
synflood	syn flood attack	TCP	☑	
portscan	port scan attack	TCP	☑	
synfrag	syn fragment attack	TCP	☐	
synfin	syn with fin attack	TCP	☐	
noflag	tcp with no flag attack	TCP	☐	
finnoack	fin without ack attack	TCP	☑	
srcsession	source session limit	TCP	☐	
winnuke	winnuke attack	TCP	☐	
land	tcp land attack	TCP	☐	
ftpovfl	ftp buffer overflow attack	TCP	☐	
smtpovfl	smtp buffer overflow attack	TCP	☐	
pop3ovfl	pop3 buffer overflow attack	TCP	☑	
url	invalid url attack	TCP	☐	
udpflood	udp flood attack	UDP	☐	
udpland	udp land attack	UDP	☐	
udpsrcsession	udp source session limit	UDP	☐	
icmpflood	icmp flood attack	ICMP	☑	
icmpfrag	icmp fragment attack	ICMP	☑	
icmpdeath	ping of death attack	ICMP	☐	
icmplarge	large icmp packet attack	ICMP	☐	

注意：攻击消息可以记录到攻击日志和邮寄给系统管理员。请见 第 37 页 “ 管理 NIDS 消息” 。

使用 CLI：

```
set nids prevention <协议_字符串> <攻击_字符串> status
{enable | disable}
```

```
set nids prevention reset
```

NIDS 预防特征说明

本节列出了 NIDS 预防特征和说明了它们所能预防的攻击类型。它还包括了一个关于系统预防攻击的动作的总体上的摘要。

NIDS 预防特征检测 TCP, UDP, ICMP 和 IP 协议的数据包中的异常部分。

特征在如下几个表格中列出:

- 第 28 页 表 11 列出了基于 TCP 的攻击的预防特征。
- 第 29 页 表 12 列出了基于 UDP 的攻击的预防特征
- 第 29 页 表 13 列出了基于 ICMP 的攻击的预防特征
- 第 30 页 表 14 列出了基于 IP 的攻击的预防特征

表 11: TCP NIDS 预防特征

特征名称	特征缩写	攻击描述	FortiGate NIDS 预防
TCP SYN 淹没	synflood	攻击者发送大量的带有非法源地址的 TCP SYN 包。目标主机的缓冲区被填满并且停止对后来的服务请求作出响应。	当每秒的 SYN 包数量超过了临界值的时候，FortiGate 设备将开始代理 TCP 会话。如果 FortiGate 代理在达到超时时间之前无法接收到对它的 SYN+ACK 消息的响应，它将阻塞这个会话。当 SYN 请求是发送到目的地址的全部端口上的时候，这个临界值四倍于它只发送到一个端口的情况。
TCP 扫描	portscan	攻击者向目标的不同端口发送数据包，以找出目标的开放的端口。	攻击者将被 FortiGate 设备所阻塞。
TCP SYN/Frag	synfrag	攻击者在一个包的片段中发送 SYN。目标主机接收这个包并等待重组。当目标主机接收到更多的 SYN 包片段时它的缓冲区被填满并停止响应服务请求。	FortiGate 设备将丢弃这个数据包。
TCP SYNFIN	synfin	攻击者在同一个数据包中同时设置 SYN 和 FIN 标志，判断目标操作系统的指纹，为随后的攻击做准备。	FortiGate 设备将丢弃这个数据包。
TCP 无标志	noflag	也称做空扫描攻击。攻击者发送将全部标志位都置零的数据包，于是目标响应一个 TCP RST （复位）包，并给出源地址和端口。	FortiGate 设备将丢弃这个数据包。
TCP FIN/NOACK	finnoack	也称做扫描攻击。攻击者发送一个将 FIN 标志设置为无应答的 TCP 包。许多操作系统会对此响应一个带有源地址和端口的 RST 包。	FortiGate 设备将丢弃这个数据包。
TCP 源会话	srcsession	攻击者建立大量的会话，增加目标的 CPU 使用率。	FortiGate 设备将丢弃这个数据包。
TCP Winnuke	winnuke	攻击者向一台运行 WIDOWS 操作系统（通常是 NETBIOS 139 端口）的目标发送超出边界的数据 （OOB），从而使系统崩溃。	FortiGate 设备将丢弃这个数据包。

表 11：TCP NIDS 预防特征 （续）

特征名称	特征缩写	攻击描述	FortiGate NIDS 预防
TCP Land	land	攻击者发送以目标的 IP 地址作为源地址的 TCP SYN 数据包，导致目标陷入循环。	FortiGate 设备将丢弃这个数据包。
FTP 溢出	ftpovfl	攻击者发送一个带有大于 478 字节的参数的命令，导致目标主机的缓冲区溢出，从而使攻击者可以获权访问特定的命令 （例如 DELE，MDTD，XMKD，RNRF 和 SIZE）。然后攻击者在目标主机上放入一个脚本以获得 ROOT 用户权限。	FortiGate 设备将丢弃数据包并复位连接。如果攻击的频率超过了临界值，FortiGate 设备将阻塞攻击者。
SMTP 溢出	smtpovfl	很多 SMTP 服务器都可能产生缓冲区溢出，并且一些 SMTP 命令可能威胁到服务器的性能或者导致目标主机崩溃。	FortiGate 设备将丢弃数据包并复位连接。如果攻击的频率超过了临界值，FortiGate 将阻塞攻击者。
TCP 非法 URL	url	攻击者对一个单独的 URL 地址发送 get 请求数据包，增加目标主机的 CPU 使用率。	FortiGate 设备将丢弃数据包并复位连接。如果攻击的频率超过了临界值，FortiGate 将阻塞攻击者。
TCP POP3 溢出	pop3ovfl	攻击者发送一个长度超过 258 字节的用户名，导致目标主机崩溃。	FortiGate 设备将丢弃数据包并复位连接。如果攻击的频率超过了临界值，FortiGate 将阻塞攻击者。

表 12：UDP NIDS 预防特征

特征名称	特征缩写	攻击描述	FortiGate NIDS 预防
UDP 淹没	udpflood	攻击者对目标主机的任意端口发送 UDP 包。如果在这个端口没有应用程序监听，目标主机将发送一个目的地不可达的 ICMP 包到源地址，通常就是目的网络的广播地址。攻击者通过发送类似的数据包增加目标的 CPU 使用率。	FortiGate 将阻塞攻击者。
UDP Land	udpland	类似于 TCP Land 攻击。攻击者发送以目标的 IP 地址作为源地址的 UDP 包，导致目标主机陷入循环。	FortiGate 将阻塞攻击者。
UDP 超量会话	udpsrcsession	攻击者向目标主机发送大量的 UDP 会话，耗尽系统资源。	FortiGate 设备将丢弃数据包。

表 13：ICMP NIDS 预防特征

特征名称	特征缩写	攻击描述	FortiGate NIDS 预防
ICMP 淹没	icmpflood	攻击者通常使用这一攻击手段结合分布式拒绝服务 （DDoS）攻击来耗尽 ISP 的带宽。攻击者首先作为一个管理者获得大量主机的控制权，然后用这些主机作为代理，让它们运行同一目的的脚本。攻击者发送大量 ICMP 响应请求，使得目标主机在试图发送响应回复的时候系统资源超载。	FortiGate 设备将阻塞攻击者。

表 13: ICMP NIDS 预防特征 （续）

特征名称	特征缩写	攻击描述	FortiGate NIDS 预防
ICMP 片段	icmpfrag	ICMP 包很少有被分割的。攻击者使用这一弱点来获取访问权或者进行拒绝服务 （DoS）攻击。	FortiGate 设备将丢弃数据包。
ICMP Death	icmpdeath	攻击者发送大于 65535 字节的 ICMP 包，导致目标主机崩溃，死机或者重新启动。	FortiGate 设备将丢弃数据包。
大型 ICMP	icmplarge	攻击者通过从多个代理处发送大尺寸的 ICMP 包耗尽 ISP 或网络服务器的带宽。	FortiGate 设备将丢弃数据包。
ICMP Sweep	icmpsweep	攻击者对网络中的不同的主机发送 echo 请求数据包。攻击者使用 echo 回复来了解目标网络的结构或者探测活动的 IP 地址。	FortiGate 设备将阻塞攻击者。
ICMP 超量会话	icmpsrcsession	对于单一主机，攻击者发送超过临界值的 ICMP 请求数据包。	FortiGate 设备将丢弃数据包。
ICMP Land	icmpland	类似于 TCP Land 攻击。攻击者发送使用目标主机的 IP 地址作为源 IP 地址的 ICMP 包，导致目标主机陷入循环。	FortiGate 设备将丢弃数据包。

表 14: IP NIDS 预防特征

特征名称	特征缩写	攻击描述	FortiGate NIDS 预防
IP 记录路由选项	iprr	用来描绘目标网络的拓扑结构。攻击者使用 IP 选项 7 （记录路由）来跟踪数据包通过一个网络时经过的地址。	FortiGate 设备将丢弃数据包。
IP 严格源记录路由选项	ipssrr	用来对抗基于 IP 地址的认证处理。攻击者使用 IP 选项 9 （严格的源路由）跟踪数据包传输时通过的地址。	FortiGate 设备将丢弃数据包。
IP 松散源记录路由选项	iplsrr	提供路由信息。攻击者使用 IP 选项 3 （松散源路由）使得数据包可以使用任何中间网关达到路由的下一个 IP 地址。	FortiGate 设备将丢弃数据包。
IP 流选项	ipstream	类似于一个访问攻击。攻击者使用 IP 选项 8 （SATNET 流识别符），它使得不被支持的 16 比特 SATNET 流识别符可以通过一个网络。	FortiGate 设备将丢弃数据包。
IP 安全选项	ipsecurity	攻击者使用 IP 安全选项使得主机发送安全信息。攻击者可以使用这些信息进行访问攻击。	FortiGate 设备将丢弃数据包。
IP 时间标记选项	iptimestamp	攻击者使用 IP 选项 4 （时间标记）来跟踪一个数据包到达目的地的时间。攻击者通过综合这个信息和路由记录信息可以描绘出网络的拓扑结构。	FortiGate 设备将丢弃数据包。
IP 未知选项	ipunknoption	有些操作系统和防火墙易于受到这个 IP 选项的攻击，它能导致目标主机崩溃。	FortiGate 设备将丢弃数据包。
IP 未知协议	ipunknproto	IP 协议号 101 和之上的号码是保留的。带有这些协议号的数据包可能意味着网络攻击。	FortiGate 设备将丢弃数据包。

表 14: IP NIDS 预防特征 （续）

特征名称	特征缩写	攻击描述	FortiGate NIDS 预防
IP 欺骗	ipspoofing	攻击者使用使用一个受信任的 IP 地址向目的主机发送数据包，从而收集目标主机的信任关系信息，使得目标主机无法提供服务，或者直接攻击目标主机。	FortiGate 设备将丢弃数据包。
IP 片段	ipfrag	IP 片段将 IP 包分割成小于 MTU 的数据包。因为只有第一个数据包带有报头，路由器不过滤剩余的数据包。如果一个数据包带有一个小量的偏移，第一个数据包比正常值小，则意味着可能是攻击。	FortiGate 设备将丢弃数据包。
IP Land	ipland	类似于 TCP Land 攻击。攻击者发送使用目标主机的 IP 地址作为源地址的 IP 包，使目标主机陷入循环。	FortiGate 设备将丢弃数据包。

配置特征临界值

您可以修改表 15 列出的 NIDS 预防特征列表的临界值。临界值根据攻击的类型设定。对于淹没攻击，临界值是每秒收到的数据包的最大数量。对于溢出攻击，临界值是命令的缓冲区的大小。对于大型 ICMP 攻击，临界值是允许传输的 ICMP 包的大小限制。

例如，将 ICMP 淹没特征的临界值设置为 500 将允许来自同一个源地址的 500 个 echo 请求，发送到响应 echo 请求的系统。如果请求的数量是 501 或者更高，FortiGate 设备将阻塞攻击者以防止系统运行遭到破坏。

如果您输入的临界值是零或者超出了允许的范围，FortiGate 设备将使用默认值。

表 15: 带有临界值的 NIDS 预防特征

特征缩写	临界值单位	默认临界值	最小临界值	最大临界值
synflood	每秒收到的 SYN 段的最大数量	200	30	3000
portscan	每秒收到的 SYN 段的最大数量	128	10	256
srcsession	来自同一源地址的 TCP 会话初始化总数。	2048	128	10240
ftpovfl	一个 FTP 命令的最大缓冲区大小 （字节）	256	128	1024
smtpovfl	一个 SMTP 命令的最大缓冲区大小 （字节）	512	128	1024
pop3ovfl	一个 POP3 命令的最大缓冲区大小。	512	128	1024
udpflood	每秒从同一源地址接收的或者发送到同一目的地址的 UDP 包的最大数量。	1024	512	102400
udpsrcsession	来自同一源地址的 UDP 会话初始化的总数。	1024	512	102400
icmpflood	每秒从同一源地址接收的或者发送到同一目的地址的 UDP 包的最大数量。	256	128	102400
icmpsrcsession	来自同一源地址的最大 ICMP 会话初始化总数。	128	64	2048

表 15: 带有临界值的 NIDS 预防特征 （续）

特征缩写	临界值单位	默认临界值	最小临界值	最大临界值
icmpsweep	每秒来自同一源地址的 ICMP 包的最大数量。	32	16	2048
icmplarge	最大 ICMP 包大小 （字节）	32000	1024	64000

按照如下操作设置预防特征临界值：

1 进入 NIDS > 预防。

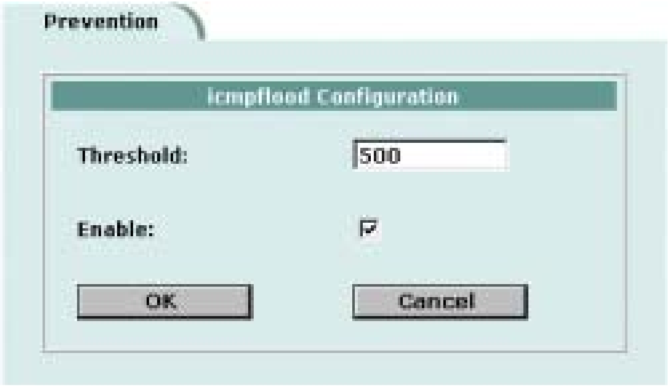
2 单击您要设置临界值的特征旁边的修改 。
不具有临界值的特征没有修改 图标。

3 输入临界值。

4 单击启用核选框。

5 单击确定。

图 6: 特征配置举例



使用 CLI：

set nids prevention <协议_字符串> <攻击_字符串> status {enable | disable}

set nids prevention <协议_字符串> <攻击_字符串> threshold <临界值_整数>

配置 syn 淹没特征值

在 SYN 淹没攻击中，攻击者向目标发送带有无效源地址的 TCP 连接请求。目标主机响应这些请求，但是因为源地址是无效的，所以作出的回应永远也不会被一台主机接收到。因此，目标主机的连接列表很快就会被填满，后来的连接将被拒绝。

为了防止 SYN 淹没攻击，FortiGate 设备监视它接收到的带有 SYN 标志的请求新连接的数据包的数量。当从单一源地址来的数据包的数量超过了临界值的时候，FortiGate 设备开始启动代理功能，它替代目标主机响应连接请求。如果 FortiGate 设备在到达超时时间之后还没有受到来自源地址的响应，于是它知道正在对付一个攻击者，并且阻塞这个连接。

值	说明	最小值	最大值	默认值
临界值	每秒发送到一个目的主机或者服务器的 SYN 请求的数量。如果 SYN 请求是发送到目的主机的全部端口的，而不是仅仅发送到一个端口，临界值将是原来的四倍。	30	3000	200
队列长度	FortiGate 设备控制的代理连接的最大数量。FortiGate 丢弃其后的代理请求。	10	10240	1024
超时	保持一个代理连接处于活动状态的以秒为单位的时间长度。这个值限制了代理连接表的大小。	3	60	15

1 进入 NIDS > **预防**。
2 对 syn 淹没特征单击修改。
3 输入临界值。
4 输入队列长度。
5 输入超时时间。
6 单击启用核选框。
或者也可以启用预防特征列表的 syn 淹没启用核选框。
7 单击确定。

使用 CLI：

```
set nids prevention tcp synflood status enable
set nids prevention tcp synflood threshold <临界值_整数>
set nids prevention tcp synflood timeout <超时_整数>
set nids prevention tcp synflood queue_size <队列长度_整数>
```

举例：NIDS 配置

预防 TCP 和 UDP 攻击

A 公司刚刚经历了一个 TCP SYN 淹没攻击，并且已经被通报说其他公司也受到了类似的 TCP 和 UDP 攻击。管理员于是想要预防这些类型的攻击对网络造成的破坏。

一般配置步骤

1 启用外部接口的 NIDS。
2 配置 TCP 和 UDP 的校验和检验。
3 启用 NIDS 预防模块。
• 启用并配置您希望 NIDS 预防模块要预防的攻击对应的 TCP 和 UDP 特征。
• 修改 syn 淹没特征的默认临界值，保持其他特征的临界值。
4 将 NIDS 配置为监视防火墙策略接受的和被监视的接口接收的通讯。
5 将 NIDS 配置为记录每个攻击的详细消息。

基于 Web 的管理程序配置步骤

1 进入 NIDS > **检测 > 一般。**

• 监视的接口：外部

• 校验和检验：TCP，UDP

• 单击应用。

1 进入 NIDS > **预防。**

• 单击左上角的启用预防。

2 单击 SYN 淹没特征的修改 。

• 临界值 : 50 (SYN/ 秒)

• 队列长度 : 500 (代理的连接)

• 超时 : 30 (秒)

• 单击启用

• 单击确定。

3 单击 synfin 特征的启用核选框。

4 对以下特征重复步骤 3：无标志 , fin 无应答 , udp 淹没。

5 进入 **日志和报告 > 日志设置。**

• 对您已经设置的日志位置单击配置策略。

• 选择攻击日志。

• 选择攻击预防。

• 单击确定。

CLI 配置步骤

1 启用外部接口的 NIDS。

```
set nids detection interface external status enable
```

2 启用对 TCP 和 UDP 的校验和检验。

```
set nids detection checksum tcp,udp
```

3 启用 NIDS 预防模块。

```
set nids prevention status enable
```

4 配置 SYN 淹没特征。

```
set nids prevention tcp synflood status enable
set nids prevention tcp synflood threshold 50
set nids prevention tcp synflood queue_size 500
set nids prevention tcp synflood timeout 30
```

5 启用以下特征：无标志，fin 无应答，UDP 淹没。

```
set nids prevention tcp noflag status enable
set nids prevention tcp finnoack status enable
set nids prevention udp udpflood status enable
```

6 将攻击消息记录到攻击日志。

```
set log policy destination {syslog | webtrends | local |
memory | console} ids status enable category prevention
```

管理 NIDS 消息

当 NIDS 检测或者预防一个攻击时，它会生成一个攻击消息。您可以将系统配置为将这个消息添加到攻击日志，并且最多可以向三个地址发送一封报警邮件。系统管理员可以使用这个信息及时地对威胁作出反应。

注意：在某些情况下，NIDS 将对同一事件生成多个 NIDS 响应消息。例如，如果同时对端口扫描启用了检测特征和预防特征，当出现一个端口扫描攻击时，将生成两个消息。您可以根据消息的各自的 ID 编号识别它们。

本节叙述了如下内容：

- 记录攻击消息日志
- 配置 FortiGate 设备发送报警邮件
- 启用 FortiGate 设备发送入侵报警邮件功能
- 定制报警邮件消息
- 减少 NIDS 攻击日志和邮件消息的数量

记录攻击消息日志

按照如下步骤将攻击消息记录到攻击日志。

1 进入**日志和报告 > 日志设置。**

2 对您已经设置的日志位置单击配置策略。

3 选择攻击日志。

4 选择攻击检测和攻击预防。

5 单击确定。

注意：关于日志消息的内容和格式的详细信息，以及日志记录的位置，请见 *日志配置和参考指南*。

使用 CLI：

```
set log policy destination {syslog | webtrends | local |
memory | console} ids status {enable | disable} category
{detection | prevention | none}
```

配置 FortiGate 设备发送报警邮件

以下操作用于配置 FortiGate 设备发送报警邮件的设置。这些设置包括 SMTP 服务器名和用户名，以及最多可以设置三个接受邮件的系统管理员的邮件地址。

按照如下步骤配置 FortiGate 设备发送报警邮件：

1 进入 **系统 > 网络 >DNS**。

2 如果还没有添加 DNS 设置，则添加您的 ISP 提供的主 DNS 服务器和辅助 DNS 服务器的地址。

因为 FortiGate 设备使用 SMTP 服务器名连接到这个邮件服务器，所以它必须要从您设置的 DNS 服务器解析这个域名。

3 单击应用。

4 进入 **日志和报告 > 报警邮件 > 配置**。

5 如果您所使用的 SMTP 服务器需要密码，则启用认证。

6 在 SMTP 服务器栏，输入 FortiGate 设备用来发送电子邮件的 SMTP 服务器名。

SMTP 服务器可以是位于连接到 FortiGate 设备的任何网络中的服务器。

7 在 SMTP 用户栏按照如下格式输入一个有效的邮件地址：user@domain.com。

这个地址出现在报警邮件的表头。

8 如果 SMTP 服务器要求的话则添加密码。

9 在电子邮件发送到栏最多可以输入三个目的邮件地址。

这是 FortiGate 设备将报警邮件实际发送到的邮件地址。

10 单击应用以保存电子邮件设置。

使用 CLI：

```
set alertemail configuration auth {enable | disable} server
<smtp-服务器_字符串> user <smtp-用户名_字符串> passwd <密码_字符串>
mailto {<电子邮件地址1_字符串> [<电子邮件地址2_字符串> [<电子邮件地址3_
字符串 >]] | none}
```

启用 FortiGate 设备发送入侵报警邮件功能

完成以下操作之后，当 NIDS 检测或者预防一次入侵时，FortiGate 设备将发送一封报警邮件。

按如下步骤启用报警邮件：

1 进入 **日志和报告 > 报警邮件 > 分类**。

2 单击启用入侵行为的报警邮件。

当 NIDS 检测或者预防一次入侵时，FortiGate 设备将发送一封报警邮件以通知系统管理员。

3 单击应用。

使用 CLI：

```
set alertemail setting option <intrusions | none>
```

定制报警邮件消息

您可以定制当 NIDS 检测或者预防入侵时发送的报警邮件消息。

按照如下步骤定制报警邮件消息：

1 进入 **系统 > 配置 > 替换消息。**

2 对邮件消息单击修改 。

服务	**名称**	**默认消息**
报警邮件	测试消息	这是测试报警邮件正文。
报警邮件	病毒消息	检测到病毒 / 蠕虫： 协议： 源 IP： 目的 IP： 发件人地址： 收件人地址：
报警邮件	入侵消息	观测到如下入侵：
报警邮件	紧急事件消息	检测到如下紧急防火墙事件：
报警邮件	硬盘满消息	日志硬盘已满。

您可以根据需要修改这些消息。消息可以是纯文本或者包含 HTML 编码。

3 单击确定以保存您所做的修改。

减少 NIDS 攻击日志和邮件消息的数量

入侵企图可能会生成大量的攻击消息。为了帮助您区分真正的警报和虚假警报，FortiGate 设备提供了减少无用的消息的数量的方法。FortiGate 设备可以根据消息生成的频率自动删除重复的消息。如果您认为您仍旧收到了过多的无用的消息，您可以手工禁用某个特征组生成消息。

自动减少消息

NIDS 生成的攻击日志和报警邮件的内容包括 ID 编号和生成这条消息的攻击的名称。这条消息中的攻击 ID 编号和名称对应于 NIDS 检测模块特征组成员列表中的 ID 编号和规则名称。

FortiGate 设备使用一个报警邮件队列来处理报警邮件，每个新的报警邮件 都将和前面的邮件相比较。如果新的消息不是重复的，FortiGate 设备将立刻发送这条消息，并将它的一个副本放入队列。如果这个新消息是一条重复消息，FortiGate 设备将删除这条消息，并在队列中相同的消息的内部计数器上加一。

FortiGate 设备将重复的电子邮件报警消息保持 60 秒。如果一条重复消息在队列中存在的时间超过了 60 秒，FortiGate 设备将删除这条消息并增加复本数量。如果副本数量大于一，FortiGate 设备将发送一个汇总邮件，在标题栏指出邮件已经重复了 x 次，在正文中说明以下邮件在过去的 y 秒中已经重复了 x 次，并包含原始消息。

手工减少消息

如果希望减少 NIDS 生成的消息的数量，您可以查看攻击日志消息和报警邮件的内容。如果有大量的消息是无效的警报 （例如，您并没有运行网页服务器，却收到了大量的网页服务器攻击警报），您可以禁用对应的攻击类型的特征组。使用攻击日志或者报警邮件中的 ID 编号可以在特征组列表中找到对应的攻击。请见 第 12 页 “ 选择一个特征组” 。

术语表

连接： 两台电脑之间、应用程序之间、进程之间或者其他诸如此类的对象之间的物理上或逻辑上的联系，或者两者都有的联系。

DMZ, 非军事区： 用来提供互联网服务而无须允许对内部（私有）网络的未经授权的访问。典型情况下，DMZ 包含了可以访问互联网的服务器，例如网页服务器 (HTTP) ，文件传输服务器（FTP）， 邮件服务器（SMTP）和域名解析服务器（DNS）。

DMZ 接口： FortiGate 上连接到 DMZ 网络的接口。

DNS，域名解析服务： 把用字母表示的节点名转换为 IP 地址的服务。

以太网：一个局域网 (LAN)，使用总线型或星型拓扑结构，支持 10Mbps 的传输速率。以太网是被广泛应用的局域网标准之一。新版本的以太网被称做 100 Base-T（或快速以太网），支持 100 Mbps 的数据传输速率。而最新的标准，千兆以太网，支持每秒 1 吉 (1,000 兆比特）的数据传输速率。

外部接口： FortiGate 连接到互联网的网络接口。

FTP，文件传输协议： 一个 TCP/IP 协议和应用程序，用于上载或下载文件。

网关： 它包括相应的软件和硬件，用来连接不同的网络。例如，TCP/IP 网络之间的网关可以连接不同的子网。

HTTP，超文本传输协议： 被万维网（WWW）所使用的协议。HTTP 定义了消息的格式和传输方式，以及服务器和浏览器应当如何对不同的命令作出响应。

HTTPS: 使用网页浏览器跨过互联网传输私人文件的 SSL 协议。

内部接口： FortiGate 用于连接到内部（私有）网络的网络接口。

互联网： 以 NFSNET 为骨干网，覆盖全球的彼此连接的网络总称。在一般的术语中，也可以表示一些互相连接的网络。

IICMP, 互联网控制信息协议：互联网协议 (IP) 的一部分。它一般被用来发送错误信息、测试数据包以及一些与 IP 有关的信息。当 PING 功能发送 ICMP 响应请求到网络中的一台主机时会用到这一协议。

IKE, 互联网密钥交换： 一种在两台安全服务器之间自动交换认证密钥和加密密钥的方法。

IMAP, 互联网消息访问协议： 一种互联网电子邮件协议，用来通过任何兼容 IMAP 的浏览器访问您的电子邮件。使用 IMAP 时，您的电子邮件保存在服务器上。

IP, 互联网协议： TCP/IP 协议的一部分，处理数据包路由。

IP 地址： 在 TCP/IP 网络中的一台电脑或者设备的识别标志。IP 地址是一个 32 比特的数字地址，通常写成用小数点分隔的四个数字。每个数字都可以是从 0 到 255 中的任何一个。

L2TP， 第二层通道协议： 点对点传输协议（PPTP）的扩展， 允许 互联网服务供应商通过它操作虚拟专用网络 (VPN)。L2TP 融合了微软公司的 PPTP 和 思科公司的 L2F 系统。要建立一个 L2TP VPN，您的互联网服务供应商的路由器必须支持 L2TP。

IPSec, 互联网协议安全： 支持 IP 层上的数据包安全交换的一组协议。 IPSec 通常用来支持 VPN。

LAN，局域网：在一个较小范围内建立的网络。大多数局域网连接工作站和个人电脑。局域网上的每个电脑都可以访问位于局域网上任何位置的任何数据和设备。这意味着大多数用户可以把他们的数据象打印机那样的物理资源一样共享。

MAC 地址，介质访问控制地址： 用来唯一识别网络上的每个节点的硬件地址。

MIB, 管理信息数据库：可以被简单网络管理协议（SNMP）网络管理程序监控的对象的数据库。

调制解调器： 可以把数字信号转换成模拟信号和把模拟信号转换成数字信号并通过电话线路传输的设备。

MTU，最大传输单元： 一个网络可以传输的数据包的最大物理尺寸，以字节为单位。任何大于 MTU 的数据包在发送之前都会被分成较小的数据包。理想情况下，网络中的 MTU 应当等于从您的电脑到目的地之间所经过的所有网络中的最小 MTU。如果您的消息大于其中的任何一个 MTU，它们会把它分割（破碎），这将会减慢传输速度。

网络掩码： 也称做子网掩码。忽略了一个完整的 IP 地址中的一部分的一组规则，从而可以无须广播就可以达到目的地址。它表示一个大的 TCP/IP 网络中的子网部分。有时用来表示一个地址掩码。

NTP，网络时间协议： 用来把一台电脑的时间同步为 NTP 服务器的时间。NTP 互联网提供精确到十毫秒以内的互联网时间（UTC）。

包： 通过包交换网络传送的消息的一部分。包的一个关键特征是它除了数据之外还包含了目的地的地址。在 IP 网络中包通常被称做数据包。

Ping，数据包互联网分组： 一个用来判定特定 IP 地址是否可以访问的工具。它的工作原理是向指定的地址发送一个数据包并等待回复。

POP3，邮局协议： 用于从邮件服务器通过互联网向邮件客户端传输电子邮件的协议。多数电子邮件客户端使用 POP 协议。

PPP，点对点传输协议： 提供了主机到网络和路由器到路由器的连接的 TCP/IP 协议。

PPTP，点对点通道协议： 基于 Windows 的建立虚拟专用网络的技术。Windows98，Windows2000 和 WindowsXP 都支持 PPTP 协议。要建立 PPTP 虚拟专用网络，您的 ISP 的路由器必须支持 PPTP。

端口： 在 TCP/IP 和 UDP 网络中，端口是逻辑连接的终点。端口号标识了端口的类型。例如，80 端口用于 HTTP 协议的数据传输。

协议： 两个设备之间商定的传输数据的格式。协议决定了要使用的错误检测的类型，数据压缩的方法（如果有的话），发送设备如何指示它完成了一个消息的发送，接收设备如何指示它已经完成了一个消息的接收。

RADIUS，远程拨号访问用户认证服务： 很多 INTERNET 服务供应商（ISP）使用的认证和计帐系统。当用户拨入一个 ISP 时，他们输入一个用户名和密码。这些信息被传送到 RADIUS 服务器，RADIUS 检验这些信息的正确性，然后授予访问 ISP 系统的权限。

路由器： 把局域往连接到互联网并为他们之间的数据提供路由的设备。

路由： 决定发送数据到目的地时要经过的路径的过程。

路由表： 含有一系列有效的数据传送路径的列表。

服务： 应答其他设备（客户）的请求的应用程序。通常用来描述任何在网络上提供类似打印、海量存储、网络访问等服务的设备。

SMTP，简单邮件传输协议： 在 TCP/IP 网络中提供邮件发送服务的程序。

SNMP，简单网络管理协议： 一组网络管理协议。SNMP 对网络的不同部分发送消息。支持 SNMP 的设备，称做代理，把他们自己的数据存储在管理信息库（MIB）中，并且把这些信息返回给 SNMP 请求的发送者。

SSH，安全命令解释器： 远程登录程序安全的替代品。您可以用它跨过网络登录到其他电脑上并执行命令。SSH 通过安全通道提供了强大的安全认证和安全通信。

子网： 网络具有相同子网地址的部分。在 TCP/IP 网络中，子网定义为所有 IP 地址前缀相同的设备。例如，所有 IP 地址从 100.100.100 开始的设备属于同一子网。从安全和性能角度考虑，把网络分割成子网是必要的。IP 网络使用子网掩码分割子网。

子网地址： IP 地址中标识子网的部分。

TCP，传输控制协议： TCP/IP 网络的主要部分之一。TCP 保证了数据的提交，也保证了数据包能够按照它们被发送时的顺序提交。

UDP，用户数据报协议： 一种无连接协议。类似于 TCP，运行于 IP 网络的顶端。与 TCP 协议不同的是，UDP 提供很少的纠错服务，取而代之的是提供了通过 IP 网络发送和接收数据报的直接传输途径。它主要用于在网络上广播消息。

VPN，虚拟专用网： 一个跨越在 INTERNET 上类似于私有网络的网络。VPN 使用加密和其它安全机制来保证只有经过认证的用户可以访问网络，并且数据不会被篡改。

病毒： 一种把自己附加到别的程序上的电脑程序，并通过这种机制在电脑中或网络上传播，通常具有有害的企图。

蠕虫： 通过电脑网络复制自己的程序或算法，通常使用电子邮件，并且会进行一些恶意的活动，例如耗尽电脑系统的资源并且可能导致系统关闭。

索引

B

报警邮件
    定制 39
    减少消息 39
    配置 38
    启用 38
    消息内容 39

D

DMZ 接口
    定义 41

F

Fortinet 客户服务 6
服务
    服务名称 9, 10

G

攻击定义
    更新 14
攻击检测
    查看特征列表 12
    概述 7
    更新攻击定义 14
    介绍 1
    校验和检验 12
    禁用 NIDS 11
    启用和禁用特征 13
    特征举例 9
    特征组 7
    选择一个特征组 12
    一般配置步骤 11
攻击类型
    拒绝服务 (DoS) 2
    NIDS 躲避 3
    权利提升 3
    嗅探 2
攻击日志
    减少消息 39
    启用 37
    消息内容 39
攻击预防
    概述 25
    介绍 1
    配置 syn 淹没特征值 32
    启用预防特征 27
    配置特征临界值 31
    一般配置步骤 26
    启用 NIDS 攻击预防 26

H

互联网密钥交换 41
HTTPS 41

I

ICMP 41
    配置验证校验和 12
IKE 41
IMAP 41
IP
    配置验证校验和 12
IPSec 41

J

技术支持 6
校验和检验
    配置 12
禁用 NIDS 11

K

客户服务 6

L

L2TP 41
路由表 42

M

MAC 地址 41
MTU 大小
    定义 42

N

NIDS
    一般配置 11
NIDS 躲避攻击 3
NIDS 检测模块 1, 7
NIDS 软件模块 1
NIDS 特性 2
NIDS 响应模块 2
NIDS 预防模块 1, 25
NTP 42

P

POP3 42
PPTP 42

Q

权利提升 3

R

RADIUS
    定义 42

S

SMTP 38
    定义 42
SNMP
    定义 42
SSH 42
SSL 41
syn 淹没特征值 32

T

TCP
    配置验证校验和 12
特征临界值 31
特征组 7

U

UDP
    配置验证校验和 12

X

嗅探攻击 2
消息
    定制报警邮件 39
    概述 37
    记录 NIDS 响应消息日志 37
    介绍 2
    减少报警邮件 13, 39
    减少日志消息 13, 39
    配置报警邮件 38
    启用报警邮件 38

Y

一般配置 11
用户定义特征
    常规配置步骤 17
    管理 24
    上载用户定义特征列表 24
    提示 17
    特征语法的细节 19
    完整的特征语法 17
    约定 17
    语法 17
用户定义特征列表
    下载用户定义特征列表 24
用户自定义特征
    创建 15
    概述 15

Z

子网地址
    定义 42
这一版本中的新增内容 3
攻击类型
    拒绝服务 （DoS）2